(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－152281
（P2002－152281A）
(43)公開日　平成14年５月24日(2002.5.24)

(51)Int.Cl.⁷		識別記号	FI			テーマコード（参考）
Ｈ０４Ｌ	12/66		Ｈ０４Ｌ	12/66	Ｂ	５Ｂ０８５
Ｇ０６Ｆ	13/00	３５１	Ｇ０６Ｆ	13/00	３５１Ｚ	５Ｂ０８９
	15/00	３３０		15/00	３３０Ａ	５Ｋ０３０
Ｈ０４Ｌ	12/28		Ｈ０４Ｌ	11/00	３１０Ｄ	５Ｋ０３３

審査請求　未請求　請求項の数12　ＯＬ　（全 13 頁）

(21)出願番号　特願2000－341926(P2000－341926)

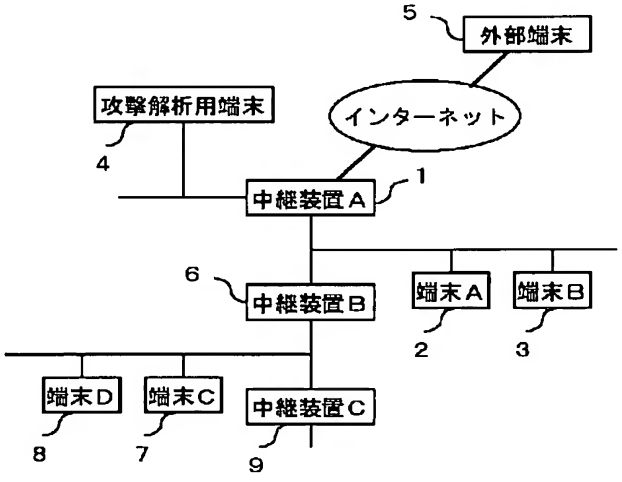
(22)出願日　平成12年11月９日(2000.11.9)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　永嶋　規充
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　後沢　忍
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100102439
弁理士　宮田　金雄　（外１名）

最終頁に続く

(54)【発明の名称】　中継装置および通信システム

(57)【要約】
【課題】　連続して不正アクセスが行われた場合の性能劣化を防ぐと共に、ネットワークに接続された端末等に不正アクセスが及ぶのを防ぐようにする。
【解決手段】　複数の端末に接続され、外部端末と上記複数の端末との通信を中継するものにおいて、複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス及びアクセス元アドレスが登録された通信制御テーブルと、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスと異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスの端末に上記通信を中継する中継制御部とを備える。



1

【特許請求の範囲】

【請求項１】　複数の端末に接続され、上記複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置において、

上記複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス及びアクセス元アドレスが登録された通信制御テーブルと、

上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスと異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスの端末に上記通信を中継する中継制御部とを備えたことを特徴とする中継装置。

【請求項２】　上記外部端末からの不正アクセスを検出した上記複数の端末のいずれかから受信した不正検出通知に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部を備えたことを特徴とする請求項１に記載の中継装置。

【請求項３】　上記外部端末からの不正アクセスを検出する不正アクセス検出部と、

上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部とを備えたことを特徴とする請求項１に記載の中継装置。

【請求項４】　上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセスの内容を記録可能な端末に上記通信を中継することを特徴とする請求項１ないし請求項３のいずれかに記載の中継装置。

【請求項５】　上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記通信のアクセス先アドレスの端末として振る舞う端末に上記通信を中継することを特徴とする請求項１ないし請求項４のいずれかに記載の中継装置。

【請求項６】　上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセスの内容を解析可能な端末に上記通信を中継することを特徴とする請求項１ないし請求項５のいずれかに記載の中継装置。

2

【請求項７】　複数の端末と、当該複数の端末に接続され、上記複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置とを備えた通信システムにおいて、

上記中継装置は、

上記複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス及びアクセス元アドレスが登録された通信制御テーブルと、

上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスと異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスの端末に上記通信を中継する中継制御部とを備えたことを特徴とする通信システム。

【請求項８】　上記端末は、上記外部端末からの不正アクセスを検出し、当該不正検出結果を上記中継装置に通知する不正検出通知部を備え、

上記中継装置は、上記端末から受信した不正検出通知に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部を備えたことを特徴とする請求項７に記載の通信システム。

【請求項９】　上記中継装置は、

上記外部端末からの不正アクセスを検出する不正アクセス検出部と、

上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部とを備えたことを特徴とする請求項７に記載の通信システム。

【請求項１０】　上記複数の端末のいずれか１つ以上の端末は、上記不正アクセスの内容を記録する不正アクセス記録部を備え、

上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセス記録部を備えた端末に上記通信を中継することを特徴とする請求項７ないし請求項８のいずれかに記載の通信システム。

【請求項１１】　上記複数の端末のいずれか１つ以上の端末は、上記中継装置の通信制御テーブルに登録されたアクセス先アドレスの端末として振る舞うように構成され、

上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセ

ス先アドレス及びアクセス元アドレスとが一致する場合に、上記中継装置の通信制御テーブルに登録されたアクセス先アドレスの端末として振る舞うよう端末に上記通信を中継することを特徴とする請求項７ないし請求項９のいずれかに記載の通信システム。

【請求項１２】　上記複数の端末のいずれか１つ以上の端末は、上記不正アクセスの内容を解析する不正アクセス解析部を備え、

上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセス解析部を備えた端末に上記通信を中継することを特徴とする請求項７ないし請求項１１のいずれかに記載の中継装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、複数の端末に接続され当該複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置と、上記複数の端末および上記中継装置を備えた通信システムとに関するものである。

【０００２】

【従来の技術】近年、インターネットの普及により、企業ネットワークをインターネットに接続するケースが多く見られる。企業ネットワークをインターネットに接続する場合、悪意のあるユーザ（クラッカーと呼ぶ）が企業ネットワークに不正にアクセスし、機密情報の漏洩、情報の改ざんが問題になってきている。

【０００３】従来、このような特定の者以外の不正アクセス者による不正アクセスや機密情報の漏洩等を防止するものとして、特開２０００－４７９８７号公報に記載されたデータ出力装置がある。

【０００４】図１２は、上記データ出力装置の構成を示す構成図である。図１２において、データ出力装置５０は、端末５７から識別情報を取得する識別情報取得手段５１と、上記識別情報に基づいてその識別情報に対応する正規データの出力を許容するか否かを判断する判断手段５４と、正規データを蓄積した正規データベース５５と、上記正規データを出力する正規データ出力手段５２と、疑似データを蓄積した擬似データベース５６と、上記疑似データを出力する擬似データ出力手段５３とで構成されている。

【０００５】上記のように構成されたデータ出力装置５０は、端末５７から取得した識別情報が正規のものであるか否かを判断手段５４において判断し、正規のものである場合には、正規データベース５５から正規データを読み出して正規データ出力手段５２より正規データを端末５７に出力する。識別情報が正規のものでない場合には、正規データとは異なる疑似データを疑似データベース５６から読み出して疑似データ出力手段５３より疑似データを端末５７に出力する。

【０００６】このようにして上記データ出力装置５０は、不正アクセス者をあたかもアクセスに成功して正規データを入手したかのような錯覚に陥らせ、不正アクセス者にアクセス失敗を悟られることなく、正規データの流出や、識別情報の解析等の不正行為を防止する。

【０００７】

【発明が解決しようとする課題】しかしながら、従来のデータ出力装置では、データ出力装置へ連続して不正アクセスがあった場合に、それぞれのアクセスに対して擬似データを出力する必要がある。したがって、この間に正規ユーザからアクセスがあった場合に、正規データの出力が遅れ、性能劣化をまねく問題があった。また、ネットワークに接続されているすべてのデータ出力装置に対して同様の不正アクセスが行われる可能性があり、セキュリティ上問題があった。

【０００８】本発明は、このような問題を解決するためになされたもので、連続して不正アクセスが行われた場合の性能劣化を防ぐと共に、ネットワークに接続された端末等に不正アクセスが及ぶのを防ぐことを目的としている。

【０００９】

【課題を解決するための手段】この発明に係る中継装置は、複数の端末に接続され、上記複数の端末以外の外部端末と上記複数の端末との通信を中継するものであって、上記複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）が登録された通信制御テーブルと、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）と異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）の端末に上記通信を中継する中継制御部とを備えたものである。

【００１０】次の発明に係る中継装置は、上記外部端末からの不正アクセスを検出した上記複数の端末のいずれかから受信した不正検出通知に基づいて、上記不正アクセスのアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）を上記通信制御テーブルに登録する不正アクセス登録部を備えたものである。

【００１１】次の発明に係る中継装置は、上記外部端末からの不正アクセスを検出する不正アクセス検出部と、上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス（宛先アドレス）及び

アクセス元アドレス（送信元アドレス）を上記通信制御テーブルに登録する不正アクセス登録部とを備えたものである。

【００１２】次の発明に係る中継装置は、上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とが一致する場合に、上記不正アクセスの内容を記録可能な端末に上記通信を中継するものである。

【００１３】次の発明に係る中継装置は、上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とが一致する場合に、上記通信のアクセス先アドレス（宛先アドレス）の端末として振る舞う端末に上記通信を中継するものである。

【００１４】次の発明に係る中継装置は、上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とが一致する場合に、上記不正アクセスの内容を解析可能な端末に上記通信を中継するものである。

【００１５】また、次の発明に係る通信システムは、複数の端末と、当該複数の端末に接続され、上記複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置とを備えたものであって、上記中継装置は、上記複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）が登録された通信制御テーブルと、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）と異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）の端末に上記通信を中継する中継制御部とを備えたものである。

【００１６】次の発明に係る通信システムは、上記端末は、上記外部端末からの不正アクセスを検出し、当該不正検出結果を上記中継装置に通知する不正検出通知部を備え、上記中継装置は、上記端末から受信した不正検出通知に基づいて、上記不正アクセスのアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）を上記通信制御テーブルに登録する不正アクセス登録部を備えたものである。

【００１７】次の発明に係る通信システムは、上記中継装置は、上記外部端末からの不正アクセスを検出する不正アクセス検出部と、上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）を上記通信制御テーブルに登録する不正アクセス登録部とを備えたものである。

【００１８】次の発明に係る通信システムは、上記複数の端末のいずれか１つ以上の端末は、上記不正アクセスの内容を記録する不正アクセス記録部を備え、上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とが一致する場合に、上記不正アクセス記録部を備えた端末に上記通信を中継するものである。

【００１９】次の発明に係る通信システムは、上記複数の端末のいずれか１つ以上の端末は、上記中継装置の通信制御テーブルに登録されたアクセス先アドレス（宛先アドレス）の端末として振る舞うように構成され、上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とが一致する場合に、上記中継装置の通信制御テーブルに登録されたアクセス先アドレス（宛先アドレス）の端末として振る舞うよう端末に上記通信を中継するものである。

【００２０】次の発明に係る通信システムは、上記複数の端末のいずれか１つ以上の端末は、上記不正アクセスの内容を解析する不正アクセス解析部を備え、上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とが一致する場合に、上記不正アクセス解析部を備えた端末に上記通信を中継するものである。

【００２１】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかる中継装置及び通信システムの好適な実施の形態を詳細に説明する。

【００２２】実施の形態１．図１は、この発明にかかる通信システムの実施の形態１のネットワーク構成を示すネットワーク構成図である。

【００２３】図１において、１は、複数の端末に接続され、当該複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置Ａである。ここでは、複数の端末として、端末Ａ２、端末Ｂ３、攻撃解析用端末４に接続されており、外部端末として、外部端末５との通信を中継する。またここでは、中継装置Ａ１と端末２～４はローカルネットワークで接続され、中継装置Ａ１と外部端末５はインターネットで接続されている。

【００２４】６は、複数の端末に接続され、当該複数の端末以外の外部端末と上記複数の端末との通信を上記中継装置Ａ１を経由して中継する中継装置Ｂである。ここでは、複数の端末として、端末Ｃ７、端末Ｄ８に接続されており、外部端末として、外部端末５との通信を上記中継装置Ａ１を経由して中継する。

【００２５】９は、図示しない複数の端末に接続され、当該複数の端末以外の外部端末と上記複数の端末との通信を上記中継装置Ａ１及び中継装置Ｂ１を経由して中継する中継装置Ｃである。

【００２６】図２は、上記通信システムの機能構成の概略を示す機能構成図である。図１と同一又は相当部分に同一符号を付し、説明を省略する。また、図２は、本実施の形態に関係する部分のみを示しそれ以外を省略して示す。

【００２７】図２において、１１は、上記複数の端末２、３のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）が登録された通信制御テーブルである。本実施の形態においては、上記アクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）に加え、さらに、不正アクセスがあった場合のアクセスの転送先アドレス（中継先アドレス）も登録されている。

【００２８】１２は、上記複数の端末２～４、７、８のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）と異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）の端末に上記通信を中継する中継制御部である。

【００２９】ここでは、上記中継制御部１２は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）と異なる端末として、通信の不正アクセスの内容を記録、解析可能であるとともに、他の端末、例えば、端末Ａ２、端末Ｂ３、端末Ｃ７又は端末Ｄ８として振る舞うことが可能に構成されている攻撃解析用端末４に通信を中継する。

【００３０】１３は、上記端末２、３、７、８から受信した不正アクセスの不正検出通知に基づいて、不正アクセスのアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）を上記通信制御テーブル１１に登録する不正アクセス登録部である。

【００３１】１４、１７、１９は、それぞれ不正アクセスを検出する不正アクセス検出部である。

【００３２】１５は、上記不正アクセス検出部１４、１７、１９で検出された不正アクセスの内容を記録する不正アクセス記録部である。

【００３３】１６は、上記不正アクセス記録部１５に記録された不正アクセスの内容を解析する不正アクセス解析部である。

【００３４】１８、２０は、それぞれ上記不正アクセス検出部１７、１９で不正アクセスが検出された場合に、不正検出通知として不正アクセスのアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）を上記中継装置Ａ１に通知する不正検出通知部である。

【００３５】ここで本発明においては、ある端末が別の端末にデータを送信する場合の宛先アドレスと送信元アドレスは、ある端末が別の端末にアクセスをする場合のアクセス先アドレスとアクセス元アドレスと同等として扱うこととし、これらを、アクセス先アドレス、アクセス元アドレスと称して説明する。

【００３６】次に、図面を参照して動作について説明する。図３は、悪意のあるユーザが外部端末５から端末Ａ２へ不正アクセスを実行し、上記端末Ａ２が上記不正アクセスを検出して、中継装置Ａ１に通知した場合の動作シーケンスである。

【００３７】外部端末５が端末Ａ２へ不正アクセスを実行すると、通信制御テーブル１１に上記外部端末５の端末Ａ２に対する不正アクセスが登録されていない場合は、上記不正アクセスのアクセスデータは中継装置Ａ１の中継制御部１１により上記中継装置Ａ１を中継して上記端末Ａ２へ伝送される（Ｓ１、Ｓ２）。

【００３８】上記不正アクセスには、例えば、次のようなものが含まれる。

（１）電子メールプロトコルSMTP(Simple Mail Transfer Protocol)のデバッグコマンドを使用し、端末Ａ２のファイルに不正にアクセスすること。

（２）ポートスキャンにより不正にアクセスを試みること。

（３）guestやroot等のめぼしいアカウント、パスワードを使用して端末Ａ２にログインを試みること。

（４）端末Ａ２に電子メールを大量に送り付け、端末やネットワークのサービスを妨害すること。

【００３９】上記端末Ａ２では、不正アクセス検出部１７が受信したアクセスデータを悪意のあるユーザからの不正アクセスがないかどうか解析する。ここでは、端末

Ａ２が受信したアクセスデータは不正アクセスであるので、上記不正アクセス検出部１７は、例えば上記（1）～（３）のような不正アクセスを検出する（Ｓ３）。上記不正アクセス検出部１７が不正アクセスを検出すると、不正検出通知部１８が上記不正アクセスの不正検出通知として不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記中継装置Ａ１に通知する（Ｓ４）。

【００４０】図４は、上記不正検出通知の一例を示す説明図である。図４において、３１は、不正検出通知を中継装置Ａ１に通知するための通信情報等が格納されたヘッダである。３２は、不正アクセスが行われた端末（ここでは、すなわち不正アクセスを検出した端末）のアドレスが格納された不正検出端末アドレスである。３３は、不正アクセスを実行した端末のアドレスが格納された不正アクセス元アドレスである。

【００４１】上記外部端末５からの不正アクセスを検出した端末Ａ２では、不正検出通知部１８が不正検出端末アドレス２２に端末Ａ２を設定し、不正アクセス元アドレス２３に外部端末５を設定し、ヘッダ２１を付与した不正検出通知を中継装置Ａ１に送信する。

【００４２】図５は、上記通信制御テーブル１１の一例を示す説明図である。図５において、不正アクセス先アドレス４１は、不正アクセスを受けた、すなわち本実施の形態では不正アクセスを検出した端末のアドレスを示す。不正アクセス元アドレス４２は、不正アクセスを実行した端末のアドレスを示す。転送先４３は、アクセスの転送先（中継先）の端末のアドレスを示す。

【００４３】上記中継装置Ａ１は、上記不正検出通知を受信すると、不正アクセス登録部１３が、上記不正検出通知に格納された不正検出端末アドレス及び不正アクセス元アドレスをそれぞれ不正アクセス先アドレス及び不正アクセス元アドレスとして、通信制御テーブル１１に登録する（Ｓ５）。

【００４４】このようにして、中継装置Ａ１は、悪意のあるユーザが外部端末５を用いて端末Ａ２へ不正アクセスを実行した場合に、通信制御テーブルに不正アクセス先アドレスおよび不正アクセス元アドレスを登録する。

【００４５】図６は、悪意のあるユーザが外部端末５から端末Ａ２へ不正アクセスを実行し、中継装置Ａ１が中継の経路を変更する場合の動作シーケンスである。

【００４６】外部端末５が端末Ａ２へ不正アクセスを実行すると、まず、不正アクセスのアクセスデータは、中継装置Ａ１に伝送される（Ｓ１）。当該中継装置Ａ１では、中継制御部１２が上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと通信制御テーブル１１に登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記アクセスデータのアクセス先アドレスと異なる端末として、攻撃解析用端末４に上記アクセスデータを中継し、一致しない場合には上記アクセスデータのアクセス先アドレスに従ってその端末に上記アクセスデータを中継する。

【００４７】ここでは、上記通信制御テーブル１１は、図５に示すように登録されているとする。このとき、上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと通信制御テーブル１１に登録されているアクセス先アドレス及びアクセス元アドレスとが一致するので、上記中継制御部１２は、中継の経路を変更し（Ｓ６）、上記アクセスデータを攻撃解析用端末４に中継する（Ｓ７）。

【００４８】上記攻撃解析用端末４は、上記中継装置Ａ１から送信されるすべてのアクセスデータを受信し、当該アクセスデータを解析して（Ｓ８）、宛先、送信元、データ種別及び受信データの内容を収集する。また、上記攻撃解析用端末４は、外部端末５からのアクセスに対して端末Ａ２として振る舞い、外部端末５に応答する（Ｓ９）。上記中継装置Ａ１は、上記攻撃解析用端末４の外部端末５に対する応答を上記外部端末５へ送信する（Ｓ１０）。

【００４９】その後、上記攻撃解析用端末４は、上記アクセスデータの解析と応答を必要に応じて繰り返し、不正アクセスの情報を収集すると共に不正アクセスの内容を解析する。

【００５０】このようにして、悪意のあるユーザが外部端末５から端末Ａ２へ不正アクセスを実行した場合に、中継装置Ａ１がアクセスデータの中継の経路を変更して、上記不正アクセスのアクセスデータを攻撃解析用端末４に転送することより、端末Ａ２およびローカルネットワーク内の他の端末、例えば、端末Ｂ３への不正アクセスを防ぐことができる。また、上記攻撃解析用端末４において、アクセスデータを記録、解析するため、不正アクセスの手順や発信元の特定に有効な情報を収集することができる。

【００５１】以上のように本実施の形態によれば、中継制御部がアクセスデータを中継する際に、上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと、不正アクセスが行われた際のアクセス先アドレス及びアクセス元アドレスが登録された通信制御テーブルとを比較して、一致する場合には上記アクセスデータのアクセス先アドレスと異なる攻撃解析用端末に上記アクセスデータを中継することにより、アクセス先アドレスの端末およびその端末に接続された他の端末への不正アクセスを防ぐことができ、セキュリティを向上させることができる。

【００５２】また、上記中継制御部は、上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと、上記通信制御テーブルに登録されたアクセス先アドレス及びアクセス元アドレスとが一致する場合には上記アクセスデータのアクセス先アドレスと異なる攻撃解析用端末に上記アクセスデータを中継し、一致しない場合には

上記アクセス先アドレスに従ってアクセスデータを中継することにより、すなわち、不正アクセスの場合はそのアクセスデータを攻撃解析用端末に中継し、正規アクセスの場合はそのアクセスデータをアクセス先アドレスに従って中継することにより、正規アクセスに応答すべき端末、例えば、端末Ａ、端末Ｂ等は、不正アクセスに応答する必要が無いので、不正アクセスに応答することによる正規アクセスへの応答の遅延等の性能劣化を防ぐことができる。

【００５３】また、本実施の形態によれば、不正アクセス登録部が不正アクセスを検出した端末から受信した不正検出通知に基づいて、不正アクセスのアクセス先アドレス及びアクセス元アドレスを通信制御テーブルに登録することにより、不正アクセスの発生に応じて通信制御テーブルを更新することができ、セキュリティを向上させることができる。

【００５４】また、本実施の形態によれば、中継装置Ａの中継制御部は、不正アクセスの内容を記録可能な上記不正アクセス記録部を備えた攻撃解析用端末に不正アクセスのアクセスデータを中継することにより、上記不正アクセス記録部に記録された不正アクセスの内容を後に解析等に利用することができるので、セキュリティを向上させることが可能となる。

【００５５】また、本実施の形態によれば、中継装置Ａの中継制御部は、不正アクセスのアクセス先アドレスの端末として振る舞うことが可能な攻撃解析用端末に不正アクセスのアクセスデータを中継することにより、不正アクセスを行った悪意のあるユーザに気づかれること無く、不正アクセスの手順や発信元の特定に有効な情報を収集することができる。

【００５６】また、本実施の形態によれば、中継装置Ａの中継制御部は、不正アクセスのアクセス先アドレスの端末として不正アクセスの内容を解析する不正アクセス解析部を備えた攻撃解析用端末に不正アクセスのアクセスデータを中継することにより、セキュリティを向上させることができる。

【００５７】なお、本実施の形態では、１つの攻撃解析用端末に不正アクセス記録部と、不正アクセス解析部と、他の端末として振る舞う機能とを備えた場合について説明したが、これに限定されるものではなく、これらの機能をそれぞれ異なる複数の攻撃解析用端末に分散して備えるようにしても良い。

【００５８】また、本実施の形態では、端末Ａが上記不正アクセスを検出して、中継装置Ａに通知するときに、上記端末Ａは不正アクセスのアクセス先アドレスとアクセス元アドレスのみを上記中継装置Ａに通知する場合について説明したが、さらに、不正アクセスの内容を上記中継装置Ａを経由し攻撃解析用端末に送信するように構成しても良い。この場合、１回目の不正アクセスの内容も上記攻撃解析用端末に記録することができるので、より多くの不正アクセスの情報を収集することが可能となる。

【００５９】また、本実施の形態では、悪意のあるユーザが外部端末から端末Ａへ不正アクセスを実行する場合について説明したが、外部端末から攻撃解析用端末へ不正アクセスを実行する場合は、攻撃解析用端末では、上記不正アクセスを検出すると、当該不正アクセスの内容を記録し、解析する。このとき上記攻撃解析用端末から中継装置Ａへの不正検出通知および中継装置Ａでの中継経路変更は不要となる。このように、不正アクセスの内容を記録または解析可能な端末に不正アクセスがあった場合は、その端末で不正アクセスの内容を記録し、解析し、中継装置Ａへの不正検出通知および中継装置Ａでの中継経路変更の処理を省略するようにしても良い。

【００６０】実施の形態２．以上の実施の形態１では、端末で不正アクセスを検出するようにしたものであるが、次に、中継装置で不正アクセスを検出する場合の実施の形態２を示す。

【００６１】本実施の形態における通信システムのネットワーク構成は、前述の実施の形態１と同様であり、説明を省略する。

【００６２】図７は、本実施の形態における上記通信システムの機能構成の概略を示す機能構成図である。図１、図２と同一又は相当部分に同一符号を付し、説明を省略する。また、図７は、本実施の形態に関係する部分のみを示しそれ以外を省略して示す。

【００６３】図７において、２１は、不正アクセスを検出する不正アクセス検出部である。中継装置で検出可能な不正アクセスとしては、例えば、次のようなものが含まれる。

（１）電子メールプロトコルSMTP(Simple Mail Transfer Protocol)のデバッグコマンドを使用し、端末Ａ２のファイルに不正にアクセスすること。

（２）ポートスキャンにより不正にアクセスを試みること。

【００６４】次に、図面を参照して動作について説明する。図８は、悪意のあるユーザが外部端末５から端末Ａ２へ上記（１）または（２）のような不正アクセスを実行し、上記中継装置Ａ１が上記不正アクセスを検出して、通信制御テーブルに登録した場合の動作シーケンスである。

【００６５】外部端末５が端末Ａ２へ不正アクセスを実行すると、当該不正アクセスのアクセスデータは、まず、中継装置Ａ１に伝送される（Ｓ１）。当該中継装置Ａ１では、中継制御部１２が上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと通信制御テーブル１１に登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記アクセスデータのアクセス先アドレスと異なる端末として、攻撃解析用端末４に上記アクセスデータを中継し、一致

しない場合には、不正アクセス検出部２１が不正アクセスの検出を行い、正規アクセスの場合に中継制御部１２が上記アクセスデータのアクセス先アドレスに従ってその端末に上記アクセスデータを中継する。

【００６６】ここでは、上記不正アクセス検出部２１が、上記外部端末５の端末Ａ２に対する不正アクセスを検出する（Ｓ３）。上記不正アクセス検出部２１が不正アクセスを検出すると、不正アクセス登録部１３が、上記不正アクセスの不正アクセス先アドレス（ここでは、端末Ａ）及び不正アクセス元アドレス（ここでは、外部端末）を通信制御テーブル１１に登録する（Ｓ５）。

【００６７】このようにして、中継装置Ａ１は、悪意のあるユーザが外部端末５を用いて端末Ａ２へ不正アクセスを実行した場合に、当該不正アクセスを検出し、通信制御テーブルに上記検出した不正アクセスの不正アクセス先アドレスおよび不正アクセス元アドレスを登録する。

【００６８】不正アクセスの不正アクセス先アドレス及び不正アクセス元アドレスを通信制御テーブル１１に登録した後に、再度、同一の不正アクセスが行われた場合の動作シーケンスは、前述の実施の形態１の図６と同様である。したがって、中継装置Ａで不正アクセスを検出した場合には、不正アクセスのアクセスデータは端末Ａに伝送されることが無いので、よりセキュリティを向上させることができる。

【００６９】以上のように本実施の形態によれば、中継装置Ａに不正アクセスを検出する不正アクセス検出部を備え、上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録することにより、前述の実施の形態の効果に加え、不正アクセスのアクセスデータは不正アクセス先アドレスの端末に伝送される前に攻撃解析用端末に伝送されるので、よりセキュリティを向上させることができる。

【００７０】なお、本実施の形態において、中継装置Ａで不正アクセスが検出された際に、さらに、不正アクセスの内容を攻撃解析用端末に送信するように構成しても良い。この場合、１回目の不正アクセスの内容も上記攻撃解析用端末に記録することができるので、より多くの不正アクセスの情報を収集することが可能となる。

【００７１】また、本実施の形態では、攻撃解析用端末に不正アクセス検出部を備え、端末Ａ及び端末Ｂに不正アクセス検出部と不正検出通知部とを備えた場合について説明したが、攻撃解析用端末から不正アクセス検出部を削除し、端末Ａ及び端末Ｂから不正アクセス検出部と不正検出通知部とを削除し、中継装置Ａのみで不正アクセスを検出するように構成しても良い。

【００７２】実施の形態３．以上の実施の形態では、悪意のあるユーザが外部端末から中継装置Ａに接続された端末へ不正アクセスを実行するものであるが、次に、外

部端末から中継装置Ｂに接続された端末へ不正アクセスを実行する場合の実施の形態３を示す。

【００７３】本実施の形態における通信システムのネットワーク構成は、前述の実施の形態１と同様であり、説明を省略する。

【００７４】図９は、上記通信システムの機能構成の概略を示す機能構成図である。図１、図２と同一又は相当部分に同一符号を付し、説明を省略する。また、図９は、本実施の形態に関係する部分のみを示しそれ以外を省略して示す。

【００７５】図９において、２２、２４は、それぞれ不正アクセスを検出する不正アクセス検出部である。

【００７６】２３、２５は、それぞれ上記不正アクセス検出部２２、２４で不正アクセスが検出された場合に、不正検出通知として不正アクセスのアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）を上記中継装置Ｂ６を経由して上記中継装置Ａ１に通知する不正検出通知部である。

【００７７】次に、図面を参照して動作について説明する。図１０は、悪意のあるユーザが外部端末５から端末Ｃ７へ不正アクセスを実行し、上記端末Ｃ７が上記不正アクセスを検出して、中継装置Ｂ６を経由し、中継装置Ａ１に通知した場合の動作シーケンスである。

【００７８】外部端末５が端末Ｃ７へ不正アクセスを実行すると、通信制御テーブル１１に上記外部端末５の端末Ｃ７に対する不正アクセスが登録されていない場合は、上記不正アクセスのアクセスデータは中継装置Ａ１および中継装置Ｂ６を中継して上記端末Ｃ７へ伝送される（Ｓ１、Ｓ１１、Ｓ１２）。

【００７９】上記端末Ｃ７では、不正アクセス検出部２２が受信したアクセスデータを悪意のあるユーザからの不正アクセスがないかどうか解析する。ここでは、端末Ｃ７が受信したアクセスデータは不正アクセスであるので、上記不正アクセス検出部２２は、不正アクセスを検出する（Ｓ３）。上記不正アクセス検出部２２が不正アクセスを検出すると、不正検出通知部２３が上記不正アクセスの不正検出通知として不正アクセスのアクセス先アドレス（ここでは、端末Ｃ）及びアクセス元アドレス（ここでは、外部端末）を上記中継装置Ｂ６を経由して上記中継装置Ａ１に通知する（Ｓ１３、Ｓ１４）。

【００８０】上記中継装置Ａ１は、上記不正検出通知を受信すると、不正アクセス登録部１３が、上記不正検出通知に格納された不正アクセス先アドレス（ここでは、端末Ｃ）及び不正アクセス元アドレス（ここでは、外部端末）を通信制御テーブル１１に登録する（Ｓ５）。

【００８１】このようにして、中継装置Ａ１は、悪意のあるユーザが外部端末５を用いて端末Ｃ７へ不正アクセスを実行した場合に、通信制御テーブルに不正アクセス先アドレスおよび不正アクセス元アドレスを登録する。

【００８２】図１１は、悪意のあるユーザが外部端末５

から端末Ｃ７へ不正アクセスを実行し、中継装置Ａ１が中継の経路を変更する場合の動作シーケンスである。

【００８３】外部端末５が端末Ｃ７へ不正アクセスを実行すると、まず、不正アクセスのアクセスデータは、中継装置Ａ１に伝送される（Ｓ１）。当該中継装置Ａ１では、中継制御部１２が上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと通信制御テーブル１１に登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記アクセスデータのアクセス先アドレスと異なる端末として、攻撃解析用端末４に上記アクセスデータを中継し、一致しない場合には上記アクセスデータのアクセス先アドレスに従ってその端末に上記アクセスデータを中継する。

【００８４】ここでは、上記通信制御テーブル１１は、不正アクセス先アドレス４１に端末Ｃ、不正アクセス元アドレス４２に外部端末、転送先４３に攻撃解析用端末が登録されているとする。このとき、上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと通信制御テーブル１１に登録されているアクセス先アドレス及びアクセス元アドレスとが一致するので、上記中継制御部１２は、中継の経路を変更し（Ｓ６）、上記アクセスデータを攻撃解析用端末４に中継する（Ｓ７）。

【００８５】上記攻撃解析用端末４は、上記中継装置Ａ１から送信されるすべてのアクセスデータを受信し、当該アクセスデータを解析して（Ｓ８）、宛先、送信元、データ種別及び受信データの内容を収集する。また、上記攻撃解析用端末４は、外部端末５からのアクセスに対して端末Ｃ７として振る舞い、外部端末５に応答する（Ｓ９）。上記中継装置Ａ１は、上記攻撃解析用端末４の外部端末５に対する応答を上記外部端末５へ送信する（Ｓ１０）。

【００８６】その後、上記攻撃解析用端末４は、上記アクセスデータの解析と応答を必要に応じて繰り返し、不正アクセスの情報を収集すると共に不正アクセスの内容を解析する。

【００８７】このようにして、悪意のあるユーザが外部端末５から端末Ｃ７へ不正アクセスを実行した場合に、中継装置Ａ１がアクセスデータの中継の経路を変更して、上記不正アクセスのアクセスデータを攻撃解析用端末４に転送することより、端末Ｃ７およびローカルネットワーク内の他の端末、例えば、端末Ａ２、Ｂ３、Ｄ８への不正アクセスを防ぐことができる。特に、中継装置Ｂ６でアクセスデータの中継の経路を変更して、攻撃解析用端末４に転送するのに比較して、よりセキュリティを向上させることができる。また、上記攻撃解析用端末４において、アクセスデータを記録、解析するため、不正アクセスの手順や発信元の特定に有効な情報を収集することができる。

【００８８】以上のように本実施の形態によれば、不正アクセスのアクセス先アドレスの端末に接続された中継

装置より上位の階層の中継装置が、不正アクセスのアクセスデータの中継経路を変更し、攻撃解析用端末に転送することにより、前述の実施の形態１の効果に加え、よりセキュリティを向上させることができる。

【００８９】なお、本実施の形態では、１つの攻撃解析用端末に不正アクセス記録部と、不正アクセス解析部と、他の端末として振る舞う機能とを備えた場合について説明したが、これに限定されるものではなく、これらの機能をそれぞれ異なる複数の攻撃解析用端末に分散して備えるようにしても良い。

【００９０】また、本実施の形態では、端末Ｃが上記不正アクセスを検出して、中継装置Ｂを経由して中継装置Ａに通知するときに、上記端末Ｃは不正アクセスのアクセス先アドレスとアクセス元アドレスのみを上記中継装置Ａに通知する場合について説明したが、さらに、不正アクセスの内容を上記中継装置Ａを経由し攻撃解析用端末に送信するように構成しても良い。この場合、１回目の不正アクセスの内容も上記攻撃解析用端末に記録することができるので、より多くの不正アクセスの情報を収集することが可能となる。

【００９１】

【発明の効果】以上のように本発明の中継装置によれば、複数の端末に接続され、上記複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置において、上記複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス及びアクセス元アドレスが登録された通信制御テーブルと、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスと異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスの端末に上記通信を中継する中継制御部とを備えたことにより、アクセス先アドレスの端末およびその端末に接続された他の端末への不正アクセスを防ぐことができ、セキュリティを向上させることができる。また、正規アクセスに応答すべき端末は、不正アクセスに応答する必要が無いので、不正アクセスに応答することによる正規アクセスへの応答の遅延等の性能劣化を防ぐことができるという効果を奏する。

【００９２】次の発明の中継装置によれば、上記外部端末からの不正アクセスを検出した上記複数の端末のいずれかから受信した不正検出通知に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部を備えたことにより、不正アクセスの発生に応じて通信制御テーブルを更新することができ、セキュリティを向上させることができるという効果を奏する。

【００９３】次の発明の中継装置によれば、上記外部端末からの不正アクセスを検出する不正アクセス検出部と、上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部とを備えたことにより、不正アクセスの発生に応じて通信制御テーブルを更新することができ、セキュリティを向上させることができる上、不正アクセスのアクセスデータは不正アクセス先アドレスの端末に伝送される前に異なる端末に伝送されるので、よりセキュリティを向上させることができるという効果を奏する。

【００９４】次の発明の中継装置によれば、上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセスの内容を記録可能な端末に上記通信を中継することにより、上記不正アクセス記録部に記録された不正アクセスの内容を後に利用することができるという効果を奏する。

【００９５】次の発明の中継装置によれば、上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記通信のアクセス先アドレスの端末として振る舞う端末に上記通信を中継することにより、不正アクセスを行った悪意のあるユーザに気づかれること無く、不正アクセスの手順や発信元の特定に有効な情報を収集することができるという効果を奏する。

【００９６】次の発明の中継装置によれば、上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセスの内容を解析可能な端末に上記通信を中継することにより、不正アクセスを解析してセキュリティを向上させることが可能となるという効果を奏する。

【００９７】次の発明の通信システムによれば、複数の端末と、当該複数の端末に接続され、上記複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置とを備えた通信システムにおいて、上記中継装置は、上記複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス及びアクセス元アドレスが登録された通信制御テーブルと、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスと異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスの端末に上記通信を中継する中継制御部とを備えたことにより、アクセス先アドレスの端末およびその端末に接続された他の端末への不正アクセスを防ぐことができ、セキュリティを向上させることができる。また、正規アクセスに応答すべき端末は、不正アクセスに応答する必要が無いので、不正アクセスに応答することによる正規アクセスへの応答の遅延等の性能劣化を防ぐことができるという効果を奏する。

【００９８】次の発明の通信システムによれば、上記端末は、上記外部端末からの不正アクセスを検出し、当該不正検出結果を上記中継装置に通知する不正検出通知部を備え、上記中継装置は、上記端末から受信した不正検出通知に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部を備えたことにより、不正アクセスの発生に応じて通信制御テーブルを更新することができ、セキュリティを向上させることができるという効果を奏する。

【００９９】次の発明の通信システムによれば、上記中継装置は、上記外部端末からの不正アクセスを検出する不正アクセス検出部と、上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部とを備えたことにより、不正アクセスの発生に応じて通信制御テーブルを更新することができ、セキュリティを向上させることができる上、不正アクセスのアクセスデータは不正アクセス先アドレスの端末に伝送される前に異なる端末に伝送されるので、よりセキュリティを向上させることができるという効果を奏する。

【０１００】次の発明の通信システムによれば、上記複数の端末のいずれか１つ以上の端末は、上記不正アクセスの内容を記録する不正アクセス記録部を備え、上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセス記録部を備えた端末に上記通信を中継することにより、上記不正アクセス記録部に記録された不正アクセスの内容を後に利用することができるという効果を奏する。

【０１０１】次の発明の通信システムによれば、上記複数の端末のいずれか１つ以上の端末は、上記中継装置の通信制御テーブルに登録されたアクセス先アドレスの端末として振る舞うように構成され、上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びア

クセス元アドレスとが一致する場合に、上記中継装置の通信制御テーブルに登録されたアクセス先アドレスの端末として振る舞うよう端末に上記通信を中継することにより、不正アクセスを行った悪意のあるユーザに気づかれること無く、不正アクセスの手順や発信元の特定に有効な情報を収集することができるという効果を奏する。

【０１０２】次の発明の通信システムによれば、上記複数の端末のいずれか１つ以上の端末は、上記不正アクセスの内容を解析する不正アクセス解析部を備え、上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセス解析部を備えた端末に上記通信を中継することにより、不正アクセスを解析してセキュリティを向上させることが可能となるという効果を奏する。

【図面の簡単な説明】

【図１】　実施の形態１におけるネットワーク構成を示すネットワーク構成図である。

【図２】　実施の形態１における通信システムの機能構成の概略を示す機能構成図である。

【図３】　実施の形態１において、不正アクセスを検出し、通知した場合の動作シーケンス図である。

【図４】　不正検出通知の一例を示す説明図である。

【図５】　通信制御テーブルの一例を示す説明図である。

【図６】　実施の形態１において、中継の経路を変更する場合の動作シーケンス図である。

【図７】　実施の形態２における通信システムの機能構成の概略を示す機能構成図である。

【図８】　実施の形態２において、不正アクセスを検出し、通信制御テーブルに登録した場合の動作シーケンス図である。

【図９】　実施の形態３における通信システムの機能構成の概略を示す機能構成図である。

【図１０】　実施の形態３において、不正アクセスを検出し、通知した場合の動作シーケンス図である。

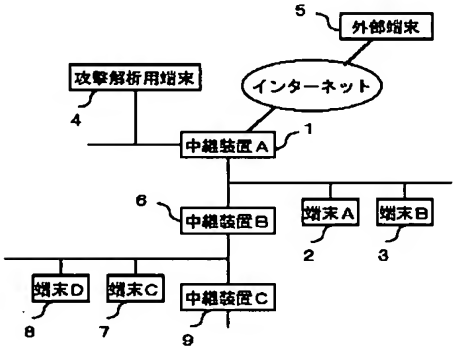
【図１１】　実施の形態３において、中継の経路を変更する場合の動作シーケンス図である。

【図１２】　従来のデータ出力装置の構成を示す構成図である。

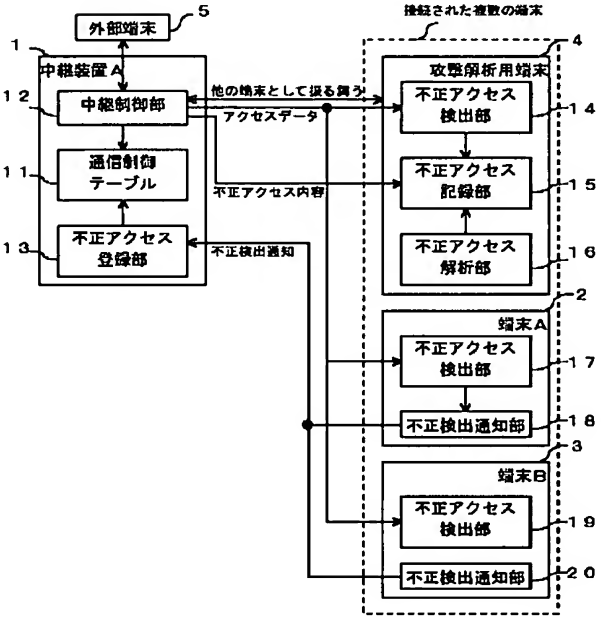
【符号の説明】

１　中継装置Ａ、　２　端末Ａ、　３　端末Ｂ、　４　攻撃解析用端末、　５外部端末、　６　中継装置Ｂ、　７　端末Ｃ、　８　端末Ｄ、　９　中継装置Ｃ、　１１　通信制御テーブル、　１２　中継制御部、　１３　不正アクセス登録部、　１４、１７、１９、２１、２２、２４　不正アクセス検出部、　１５不正アクセス記録部、　１６　不正アクセス解析部、　１８、２０、２３、２５不正検出通知部、　５０　データ出力装置、　５１　識別情報取得手段、　５２　正規データ出力手段、　５３　疑似データ出力手段、　５４　判断手段、　５５　正規データベース、　５６　疑似データベース。

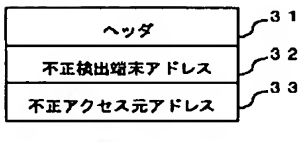
【図１】



【図２】

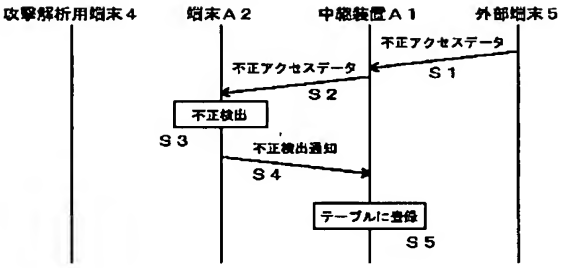


【図４】



不正検出通知のフォーマット

【図３】

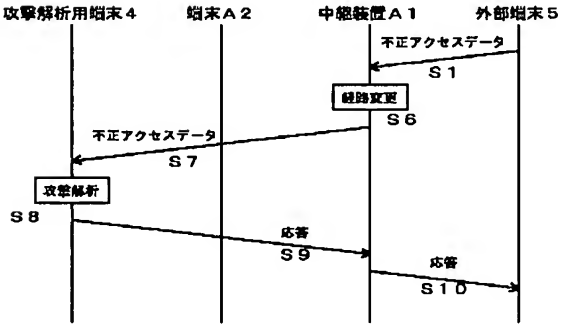


【図５】

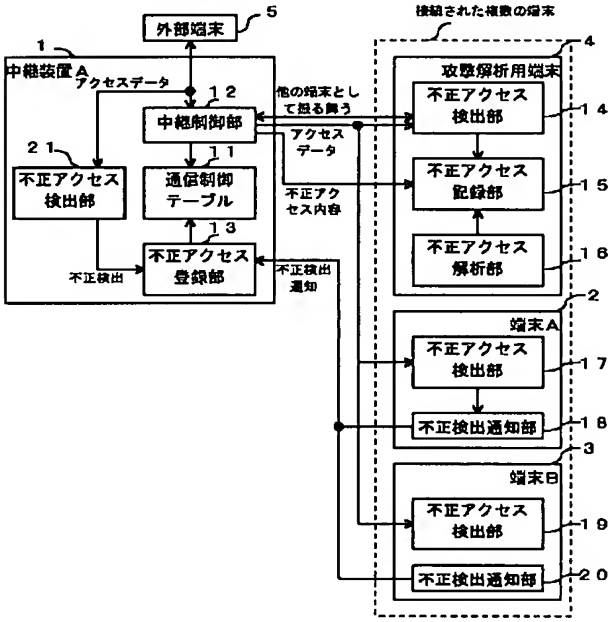
４１ 不正アクセス先アドレス	４２ 不正アクセス元アドレス	４３ 転送先
端末Ａ	外部端末	攻撃解析用端末
:	:	:
:	:	:

不正検出通知のフォーマット

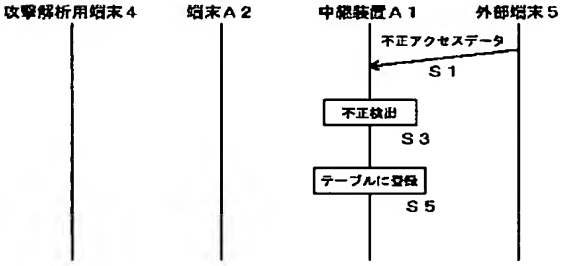
【図６】



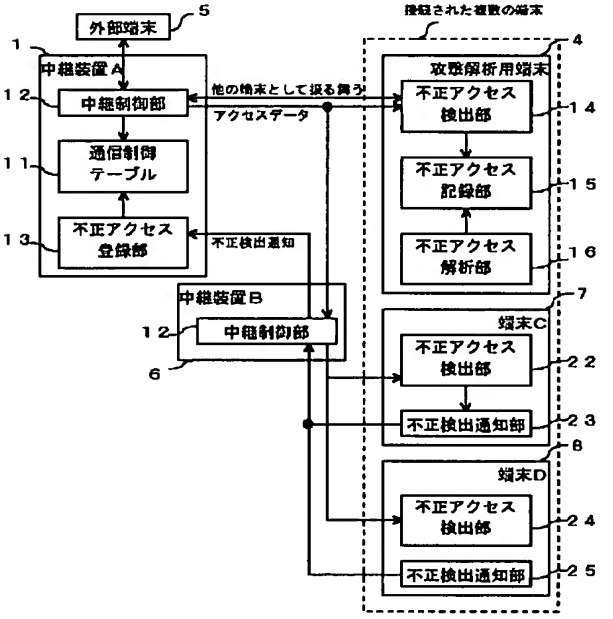
【図７】



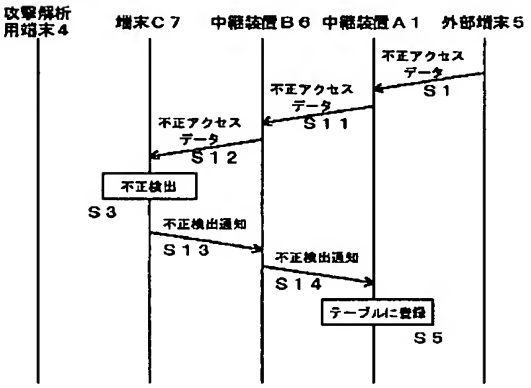
【図８】



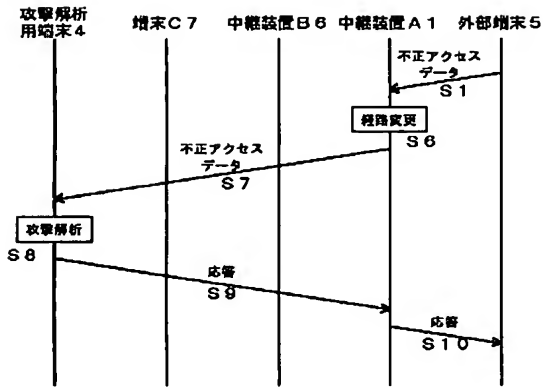
【図９】



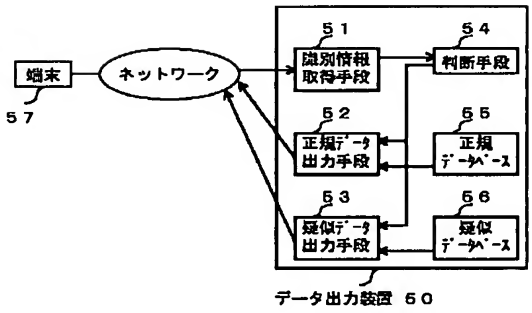
【図１０】



【図１１】



【図１２】



フロントページの続き

Ｆターム(参考)　5B085 AC03 AE01 AE06
5B089 GA21 GA31 GB02 HA10 KA17
KB13 KC34 KC52
5K030 GA15 HD03 JT02 KA04 MC08
5K033 AA08 CB08 DA01 DA06 DB18
EA06